What is claimed:

1. A method performed in a server on a network for securely authenticating to the server a user having a magnetic stripe card and a user device including a smart chip connected to a magnetic stripe reader, comprising the steps of:

a. receiving at the server information including a user device identification in a form for identifying a smart chip connected to a magnetic stripe reader and a card identification in a form for identifying a card read by said reader from a magnetic stripe on a card;

b. decrypting said user device identification and comparing the decrypted identification to records in a database to find a match;

c. comparing said card identification to records in a database to find a match; and

d. approving the user as authentic if a record matches the decrypted user device identification and that record is associated with a record that matches the card identification.

2. The method of claim 1 further comprising:

e. receiving at the server a personal identification number; and

f. comparing the received personal identification number to records in a database to find a match.

3. A method for securely authenticating to a server on a network the identity of a user having a magnetic stripe card and a user device including a smart chip, a keyboard and a magnetic stripe reader, comprising the steps of:

a. on the user device, receiving at the magnetic stripe reader a card identification read from a magnetic stripe on a card and transmitting said card identification to the server;

b. on the user device, transmitting from the smart chip to the server a user device identification;

c. on the user device, receiving at the keyboard an entered personal identification number;

d. on the server, comparing said user device identification to records in a database to find a match;

e. on the server, comparing said card identification to records in a database to find a match; and

f. approving the user as authentic if a record that matches the user device identification is associated with a record that matches the card identification, and the personal identification number satisfies a processing requirement.

4. The method of claim 3 wherein the user device identification is encrypted for decryption by the server.

5. The method of claim 3 wherein the processing requirement matches a personal identification number to a data record.

6. The method of claim 3 wherein the processing requirement is a function of information read by the magnetic stripe reader.

7. The method of claim 3 wherein the personal identification number is processed in the smart chip.

8. The method of claim 3 wherein the personal identification number is transmitted to the server and processed in the server.

9. A method for securely authenticating a user to a server on a public network performed in a user device including a smart chip, a keyboard and a magnetic stripe reader, comprising the steps of:

a. receiving at the magnetic stripe reader information read from a magnetic stripe on a card;

b. receiving at the keyboard an entered personal identification number; and

c. processing the personal identification number and, if it satisfies a processing requirement which is a function of information read from the magnetic stripe, transmitting from the smart chip to the server across the public network an encrypted user device identification code for identifying the smart chip to the server.

10. The method of claim 9 wherein the user device is human portable.

11. The method of claim 9, further comprising:

d. requesting an electronic cash transaction with a server; and downloading electronic cash into the smart chip in the user device.

12. The method of claim 9, further comprising:

d. processing the information read from the magnetic stripe and, if it does not satisfy a processing requirement, reaching a result of failure to authenticate.

13. The method of claim 9, further comprising:

d. receiving other information to be processed and forwarding said information to the server along with the encrypted user device identification code for identifying the smart chip to the server.

14. A method for securely authenticating a user to a server on a public network performed in a user device including a smart chip, a keyboard and a magnetic stripe reader, comprising the steps of:

a. receiving at the magnetic stripe reader information read from a magnetic stripe on a card;

b. receiving at the keyboard an entered personal identification number; and

c. processing the personal identification number and, if it satisfies a processing requirement which is a function of information stored within the smart chip, transmitting from the smart chip to the server across the public network information read from the magnetic stripe with an encrypted user device identification code for identifying the smart chip to the server.

15. The method of claim 14 wherein the user device is human portable.

16. The method of claim 14, further comprising:

d. processing within the smart chip the information read from the magnetic stripe and, if it does not satisfy a processing requirement, reaching a result of failure to authenticate.

17. The method of claim 14, further comprising:

d. receiving other information to be processed by the server and transmitting it to the server.

18. The method of claim 14, further comprising:

d. receiving a second personal identification number and transmitting it to the server.

19. A method for securely authenticating a user to a server on a public network performed in a user device including a smart chip, a keyboard and a magnetic stripe reader, comprising the steps of:

a. receiving at the magnetic stripe reader information read from a magnetic stripe on a card;

b. processing the information read from the magnetic stripe and, if it satisfies a processing requirement, transmitting from the smart chip to the server across the public network an encrypted user device identification code for identifying the smart chip to the server.

20. The method of claim 19, further comprising:

d. receiving other information to be processed by the server and transmitting it to the server.

21. The method of claim 19, further comprising:

d. receiving a personal identification number and transmitting it to the server.

22. The method of claim 19, further comprising:

d. receiving a personal identification number; and

e. processing the personal identification number and, if it does not satisfy a processing requirement, reaching a result of failure to authenticate.

23. The method of claim 19 wherein the user device is human portable.

24. The method of claim 19, further comprising:

d. requesting an electronic cash transaction with a server; and downloading electronic cash into the smart chip in the user device.